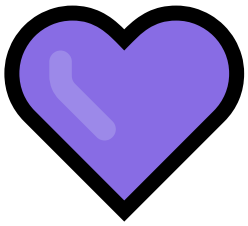
Learn Cyber Safety Basics



The complete guide by

CyberShoulder

(2025 - Edition 001)

Contents

This document “Learn Cyber Safety Basics (2025 – E001)” is available at:

https://cybershoulder.org/paper-content

📜 Sharing & Use

Learn Cyber Safety Basics is created by *Cyber Shoulder* — a community-driven initiative that believes cyber safety should be simple, shareable, and accessible to everyone.

You are **welcome to print, share, and distribute** this guide in your workplace, school, community group, or at home — anywhere it might help someone feel safer and more confident online.

You may not sell or alter it for profit, but you can:

- Print or photocopy it for personal or group learning
- Share the digital file freely
- Quote information freely

This guide was written to be *shared*, not stored.
If it helps one person spot a scam or feel calmer online — it's done its job.

🧭 About Cyber Shoulder

Cyber Shoulder exists to make online safety feel human — friendly advice for everyday people, not tech experts. We focus on *confidence, kindness, and community* as the foundation of cyber awareness.

You'll find more free resources on our website: 🌐 **www.cybershoulder.org**

Explore:

- ❔ **Advice** — Simple, jargon-free guidance for individuals and small businesses.
- 📄 **Paper Content** — Free printable posters and guides (like this one).
- 🎙️ **Broadcasts** — Our podcast, *Cyber Shoulder*, featuring stories, hot takes, and honest conversations about security.
- 🧰 **Tools** — Practical resources for spotting scams, checking exposure, and protecting your data.
- 💬 **Forum** — A friendly community space to ask questions and share experiences.

Cyber Shoulder
United Kingdom
🌐 www.cybershoulder.org
✉️ info@cybershoulder.org

Printed and shared with care. 💜

💙 Learn Cyber Safety Basics

A friendly guide to feeling confident, safe, and in control online.

What This Document Is

This isn't a technical manual — it's a collection of short, simple lessons to help you build cyber confidence step by step. Each section explains a key topic (like passwords, scams, or online sharing) in clear, everyday language. You'll learn what to look out for, how to protect yourself, and what to do if something goes wrong.

🎯 Why It Exists

Cyber safety shouldn't feel scary or exclusive. Everyone deserves to understand how to protect themselves online, even without technical experience.

CyberShoulder exists to make that easier — friendly, practical, and judgment-free.

Most online threats rely on *tricking trust*, not breaking technology. This guide helps you stay aware, protect that trust, and still enjoy the internet.

📝 What You'll Learn

Across these pages, you'll discover how to:

- ✅ Create and manage stronger passwords
- ✅ Recognise scams, fake messages, and risky links
- ✅ Keep your devices updated and backed up
- ✅ Control what you share and who can see it
- ✅ Support friends or family who might be unsure
- ✅ Stay calm and act quickly if something feels wrong

How to Use This Workbook

- Take it **one topic at a time.** There's no rush — each page builds your confidence.
- Use the **Q&As** to test your understanding (answers are explained).
- Highlight or tick progress boxes as you go.
- Revisit sections — good habits get stronger with practice.

💬 **Tip:** Cyber safety isn't about perfection. It's about recognising when something doesn't look right — and knowing what to do next.

Who This Guide Is For

This guide is for *everyone* who uses the internet — at home, at work, or on the go. It's written for real people, not IT professionals. Whether you're helping a family member, teaching a class, or just improving your own safety, these pages are for you.

Our Promise

This guide exists purely to inform, not to sell or collect anything. Use it freely, copy it, teach from it, and pass it on.

Confidence Scale

In regards to Cyber safety, circle where you feel you are today:

1 I'm still learning the basics.
2 I know some key steps but forget them sometimes.
3 I use good habits most of the time.
4 I feel calm and capable when something looks suspicious.
5 I'm confident enough to help others.

Section 1:

Passwords & Logins

Build your first line of defence.

Understanding Passwords

Every account you own — email, shopping, banking, social media — is protected by a password. It's your digital key, and if someone else gets it, they can open that door too.

Attackers know this. They spend their time collecting and testing passwords.
They don't "hack" like in the movies — they *guess smartly* using leaked information, patterns, and tools.

What Makes a Password Strong?

Factor	Weak Example	Strong Example	Why It Matters
Length	Dog123	BlueRiverWindow	Longer = harder to brute-force.
Predictability	Password!	BridgeMoonCoffee	Random words beat clever tricks.
Reuse	Same everywhere	Unique for each site	Stops one breach spreading.
Storage	Sticky note	Password manager	Keeps passwords private and encrypted.

Remember: Three or four random words make a password both *memorable* and *nearly uncrackable*.

💣 How Passwords Get Guessed or Stolen

🧱 1. Brute Force

They use software that tries every possible combination of letters, numbers, and symbols. Short passwords fall instantly — long ones take years or centuries to crack.

📜 2. Credential Leaks

When a website gets hacked, attackers often steal its user database — including passwords. Those passwords are then sold or shared online. Criminals try them on *other* sites to see what else works — a method called **credential stuffing**.

If you reuse the same password for multiple sites, one leak opens all of them.

🔍 3. Guessing Based on You

Attackers look at your social media or public info. Birthdays, pet names, football teams — anything visible online can end up in a password guess list.

Example:
You post “Can’t believe Daisy’s 3 today!”
Attackers try passwords like Daisy3, Daisy2024, or MyDogDaisy!.

💬 4. Phishing

Instead of guessing, attackers *ask you directly* — they send fake emails or messages that look like your bank, workplace, or delivery company. They lead you to a fake login page and record what you type.

You think you’re signing into your account — but you’ve just given your password away.

⚙️ 5. Malware or Keyloggers

Sometimes, if a computer or phone is infected, the malware watches what you type and steals your credentials silently. That’s why **device updates and antivirus software** matter just as much as strong passwords.

🔐 Why “P@ssw0rd!” Isn’t Clever

Attackers expect symbol swaps like @ for “a” or 0 for “o”. They include them in their cracking lists automatically.

So P@ssw0rd! can be guessed almost instantly but OrangeRiverCloud! would take thousands of years to break — and it’s easier to remember.

🧩 Password Managers

A **password manager** is like a digital safe for your logins. It stores unique, strong passwords for every site, encrypted behind one master password.

✅ Creates long random passwords for you
✅ Fills them in safely on the right site
✅ Works across your phone and computer

If you remember one strong master password, you never need to remember the rest.

📦 Multi-Factor Authentication (MFA)

Even the best passwords can be stolen — MFA makes that useless. It’s a second check, like a code texted to your phone or a tap in an app that confirms “yes, this is me.”

Turn it on for your **email, banking, and social media** first.
Those are your digital keys — if they’re secure, everything else is too.

Learn & Try

Q1 – Which of these is strongest?

A. Summer2024
B. P@ssword!
C. BlueRiverWindow
D. 12345678

Q2 – Which login habit is safest?

A. Use one strong password for all sites
B. Write them in a notebook
C. Use a password manager
D. Memorise them all

Q3 – What does MFA do?

A. Replaces passwords
B. Adds a second check before access
C. Makes passwords longer
D. Only works for work accounts

Quick Wins

✅ Use **three random words** for each password.
✅ **Turn on MFA** for your key accounts.
✅ **Use a password manager** to store them securely.
✅ **Update reused passwords** today — start with email and banking.
✅ Keep your devices updated and scan for malware regularly.

Confidence Check

☐ I know how attackers guess passwords.
☐ I've stopped reusing the same password.
☐ I've turned on MFA.
☐ I've tried or plan to try a password manager.

Section 2:

Scams & Phishing

Learn how scams trick people — and how to stop them before they start.

Understanding Scams

Scams are built to *rush, scare,* or *reassure* you into acting fast. They often arrive as emails, texts, or calls pretending to be someone you trust — your bank, a courier, even a friend.

The goal is simple: make you react before you think. They succeed because they target **emotions, not intelligence**. Even careful, educated people get caught when tired, distracted, or stressed.

How Scammers Trick You

Tactic	Example	What They're Doing
Urgency	"Act now or your account will close!"	Stops you from pausing to think.
Fear	"There's a problem with your payment."	Pushes panic to get compliance.
Reward	"You've won a prize — click here!"	Hooks curiosity and greed.
Familiarity	"Hi Mum, it's me — new number!"	Pretends to be someone you know.
Authority	"This is the police / your bank calling."	Uses trust in official titles.

Remember: If a message makes you *feel*, it's trying to make you *act*.

How Phishing Works

Phishing is when scammers send fake messages to steal information.
They copy logos, wording, and sender names so well that even experts can hesitate.

Here's what usually happens:

1. You get a message with a link or attachment.
2. It leads to a fake website that looks real.
3. You log in — and they steal your password.

Once they have access, they:

- Try the same password on your other accounts.
- Send new phishing messages from *your* inbox.
- Lock you out and demand payment to restore access.

Spot the Red Flags

🔔 Warning Sign	What It Means
The email address looks almost right	e.g. support@micr0soft.com instead of microsoft.com.
There's pressure to act quickly	"Limited time only" or "confirm within 24 hours."
The link looks strange	Hover over it — does it match the real site?
Unexpected attachments	Don't open unless you're expecting them.
Generic greetings	"Dear user" instead of your name.
Spelling or design errors	Quick giveaways of fake sites.

💡 **Tip:** If something feels odd, it usually is.
Go directly to the website or app — never through the link.

Real-World Examples

Below are two examples of real scam messages that have been sent to people in the UK.

They look convincing at first glance, but each one contains clear warning signs once you know what to look for. Take a moment to read them, spot the clues, and compare with the safe responses shown underneath.

Example 01

Subject: "Delivery Attempt Failed — Schedule Again"
From: RoyalMail-Notice@post-alert.co.uk
Message:

"We tried to deliver your parcel. Please pay £1.99 to reschedule delivery."

Spot the issues:

- The sender isn't from the real Royal Mail domain.
- The link is shortened (hides the real address).
- Royal Mail never charges to redeliver.

✅ **Correct response:** Delete it or forward to report@phishing.gov.uk.

Example 02

Subject: "Unusual Sign-In Attempt Detected"
From: security@micr0soft-support.com
Message:

"We noticed a new sign-in to your account from London, UK.
If this wasn't you, please verify your account immediately to avoid suspension."

Spot the issues:

- The sender address looks right but includes a **zero (0)** instead of an "o" — micr0soft-support.com is fake.
- The message uses **fear and urgency** to make you click quickly.
- The **real Microsoft** would direct you to log in through your normal app, not a link in an email.

✅ **Correct response:** Ignore the link.

Learn & Try

Q1 — Which message is most likely a scam?

A. “Your bank will never ask for passwords by email.”
B. “Urgent: Confirm your bank details now to avoid account closure.”
C. “Your monthly statement is ready in your bank app.”
D. “Reminder: You have a meeting at 3 pm.”

Q2 — What should you do with a suspicious link?

A. Click it to check where it goes
B. Forward it to friends to warn them
C. Hover to preview, then delete if it looks off
D. Reply and ask if it’s real

Q3 — What’s the safest next step if you’ve already clicked?

A. Ignore it and hope it’s fine
B. Change your password immediately
C. Click the link again to check
D. Email the scammer to apologise

Quick Wins

✅ **Pause before you click** — slow down and read carefully.
✅ **Check the sender** — official addresses only.
✅ **Don’t trust links or attachments** you weren’t expecting.
✅ **Go direct to the app or site** instead of following a link.
✅ **Report scams** by forwarding to report@phishing.gov.uk or texting **7726** (free UK).

Confidence Check

☐ I can spot a message that creates urgency or fear.
☐ I know how to check if a sender address is real.
☐ I’ve practised hovering over links before clicking.
☐ I know where to report scam emails or texts.

Section 3:

Messaging & Links

Stay safe when chatting, sharing, or clicking online.

Understanding Messaging Risks

Most scams don't arrive by email anymore — they come through your phone, social apps, and messaging platforms. From "delivery texts" to "friend links," attackers know that people trust chats more than inboxes.

Messaging scams work because they blend into normal life. They use your habits — quick replies, tapping links, or forwarding jokes — to slip through without question.

You don't need to stop using messages — just slow down before you click or reply.

Common Messaging Traps

Type	Example	Why It Works
Delivery or refund texts	"Your parcel is waiting — pay £1.99 to release it."	Creates urgency and looks routine.
"Is this you?" DMs	"You're in this video 😂"	Uses curiosity and fear of reputation.
Family or friend impersonation	"Mum, I've smashed my phone, text me here."	Exploits care and panic.
Fake prize or survey	"You've won an Amazon gift card — claim now."	Promises reward or luck.
Account security alerts	"We detected a new login — confirm details here."	Uses fear of losing access.

🔗 Spotting Risky Links

Attackers often hide danger behind normal-looking links.
Before you click, always **pause and check**:

1️⃣ **Hover** (PCs) or **press and hold** (phones) to preview the real web address.
2️⃣ **Look closely** — does it match the official site?

microsoft.com ✅ (real)
micr0soft-support.com ❌ (fake)

3️⃣ **Avoid shortened links** (bit.ly, tinyurl, etc.) — they hide where they lead.
4️⃣ **Never log in** through a link sent by message — go directly to the website or app.

Tip: If it feels urgent or unusual, don't click. Go to the app yourself instead.

📱 Real-World Example

Message: "Hey, you're in this photo! 😂 https://tinyurl.com/7g82yt"
Platform: WhatsApp

Spot the issues:

- The link is shortened (no way to see the real address).
- The message is vague but emotional — curiosity bait.
- It's a common trick used to install malware or steal login cookies.

✅ **Correct response:** Don't click. Delete the message and tell the friend their account may have been hacked.

Learn & Try

Q1 — Which of these is safest to click?

A. A link sent by a friend that says “Check this out!” with no context
B. A link to your online banking sent by text
C. A link you find by searching for the company’s website yourself
D. A shortened link from social media comments

Q2 — What should you do if a friend’s account sends a strange message?

A. Reply to ask what it is
B. Click to check before telling them
C. Ignore it and contact them another way
D. Forward it to others to warn them

Q3 — Which of these is *not* a safe sign?

A. A message asking for money or personal details
B. Messages with clear context and personal references
C. Links you can verify independently
D. Accounts that use official domains (e.g. @nhs.uk)

Quick Wins

✅ **Pause before you tap.** Most scams rely on speed, not skill.
✅ **Check the link** by hovering or pressing and holding.
✅ **Don’t forward chain messages** — they spread misinformation.
✅ **Use official apps** instead of links in chats.
✅ **Report suspicious messages** to your messaging platform or phone provider.

Confidence Check

☐ I can spot when a message is suspicious.
☐ I know how to check where a link really goes.
☐ I avoid clicking shortened or strange URLs.
☐ I know how to report or block suspicious accounts.

Section 4:

Device & Data Care

Protect the devices and information you rely on every day.

Understanding Device Safety

Your phone, tablet, and computer are the gateways to your digital life. If one becomes infected or out of date, attackers can slip through the gaps — even if your passwords are strong.

Device care isn't about being technical; it's about small habits that keep things running safely. Think of it like brushing your teeth — short, regular maintenance prevents big problems later.

Keep Software Updated

Updates don't just add new features — they fix security holes.
Every update you skip gives criminals more time to exploit old flaws.

Do this:
✅ Turn on *automatic updates* for your operating system, browser, and apps.
✅ Restart your device regularly so updates finish installing.
✅ Update antivirus and security tools at the same time.

💡 *Tip:* If an update notification looks odd or asks for payment, ignore it and open your settings manually.

Be Careful What You Install

Malware often hides inside fake apps, free tools, or attachments.
It can record your keystrokes, steal passwords, or track you silently.

Stay safe:
✅ Only download apps from official stores (Google Play, Apple App Store, Microsoft Store).
✅ Avoid "cracked" or "free premium" versions of software.
✅ Check app reviews and permissions before installing.
✅ Delete apps you don't use — fewer apps mean fewer risks.

Back Up Your Data

Backups are your safety net. If your device fails, gets stolen, or hit by ransomware, a recent backup lets you recover easily.

Options:

- **Cloud backup:** automatically saves photos and documents online (Google Drive, iCloud, OneDrive).
- **External drive:** plug in a USB drive once a week and copy important files.

🔁 *Golden rule:* at least one copy in the cloud + one copy offline.

Keep Devices Clean

Over time, devices fill with old apps, downloads, and temporary files.
These clutter not only slows things down but can hide outdated, risky software.

Once a month:
✅ Clear downloads and temporary folders.
✅ Remove unused extensions or plugins.
✅ Review browser "saved passwords" and delete any duplicates.
✅ Run a quick antivirus or security scan.

Manage Permissions & Privacy

Apps don't always need full access to your data or location.
Checking permissions keeps your information private — even from legitimate apps.

Do this:
✅ Open *Settings → Privacy / Permissions* and review access by app.
✅ Turn off camera, mic, or location for apps that don't need them.
✅ Set your device to auto-lock after a few minutes of inactivity.

💬 *Remember:* privacy isn't about hiding — it's about choosing what to share.

Learn & Try

Q1 — Why are updates important?

A. They make your device faster
B. They fix known security weaknesses
C. They remove old photos
D. They don't matter if you have antivirus

Q2 — Which backup setup is safest?

A. Files only on your laptop
B. One copy in the cloud and one on a USB drive
C. One copy emailed to yourself
D. Printing important files

Q3 — What's the risk of "free cracked" software?

A. Slower download speeds
B. You might not get updates
C. It could contain malware or spyware
D. It's legal but unstable

Quick Wins

✅ Turn on automatic updates.
✅ Back up files to cloud + drive.
✅ Install apps only from official stores.
✅ Review app permissions monthly.
✅ Run antivirus scans regularly.

Confidence Check

☐ I've enabled automatic updates.
☐ I back up my files in at least two places.
☐ I only install trusted apps.
☐ I review permissions and clean up regularly.

Section 5:

Online Privacy

Stay in control of what you share, and who can see it.

Understanding Online Privacy

Every time you post, search, or sign up online, you share a little piece of yourself — your habits, interests, and sometimes your identity.
Individually these seem harmless, but together they form a detailed picture that others can use.

Privacy isn't about hiding; it's about **choosing** what to reveal and keeping your personal life under your control.

What You Reveal Without Realising

Even simple online actions can expose more than you intend.

Example	What It Gives Away	Why It Matters
Posting a holiday photo	Your location and travel dates	Tells others your home is empty.
Sharing a work badge selfie	Workplace, department, ID details	Enables targeted phishing.
Birthday posts	Exact date of birth	Common password recovery info.
"What's your pet's name?" quizzes	Security-question answers	Used to guess login details.
Public friend lists	Your contacts and interests	Helps scammers impersonate you.

If you wouldn't share it on a public noticeboard, think twice before sharing it online.

🔒 Strengthen Your Privacy Settings

Every major platform — Facebook, Instagram, TikTok, Google, LinkedIn — has privacy controls.
They're often buried in menus, but worth finding.

Do this:

✅ Set profiles to *Friends / Contacts Only*.
✅ Limit who can tag or mention you.
✅ Review visibility of old posts and photos.
✅ Turn off "public search" so your profile doesn't appear on Google.
✅ Check who can see your phone number or email address.

🔁 *Set a reminder to review privacy settings every few months — platforms change quietly.*

📱 App & Tracking Controls

Many apps track where you go and what you do to tailor adverts.
That data can also leak if the app is insecure.

Stay private:

✅ On phones, go to *Settings → Privacy → Tracking* and turn off tracking for apps that don't need it.
✅ Restrict location access to "While Using the App."
✅ Clear browser cookies and ad IDs regularly.
✅ Use a privacy-focused browser or search engine if you prefer less data collection.

Learn & Try

Q1 — Which post shares too much?

A. “Love this new restaurant!”
B. “Finally on holiday for two weeks 🏖️”
C. “Happy birthday to my brother!”
D. “My new phone takes great photos.”

Q2 — What’s the safest setting for your social profile?

A. Public — more followers
B. Friends / Contacts Only
C. Friends of Friends
D. No restrictions

Q3 — Why are online quizzes risky?

A. They collect security-question answers
B. They’re boring
C. They take too long
D. They slow your phone

Quick Wins

✅ Review social-media privacy settings today.
✅ Remove personal details from public bios.
✅ Disable unnecessary app tracking.
✅ Think before you post — pause, then share.
✅ Use privacy-friendly browsers or extensions.

Confidence Check

☐ I know how to review my privacy settings.
☐ I understand what personal data can be used against me.
☐ I limit who can see my posts and information.
☐ I’ve turned off tracking for apps that don’t need it.

Section 6:

Helping Others

Support others in staying calm, safe, and confident online.

Why Helping Matters

Cyber safety isn't a solo skill — it's a shared one. When you help someone else avoid a scam or recover from one, you strengthen the whole community around you.

Everyone, from family to co-workers to friends, experiences online threats differently. Some people feel embarrassed, others don't know what to look for, and many just need someone to explain things simply and kindly.

Being a Cyber Shoulder means listening first, guiding gently, and never judging.

How to Talk About Cyber Safety

Situation	What Helps	Why It Works
Someone's worried they've been scammed	Stay calm, listen, and thank them for speaking up.	Reassurance stops panic and encourages honesty.
They clicked a link or shared details	Help them change passwords and report it right away.	Focus on solutions, not blame.
They say "I'm not good with tech"	Offer to show, not tell — sit beside them.	Builds confidence through learning by doing.
A young person overshares online	Ask questions like "Who can see that?" instead of giving orders.	Promotes thinking instead of resistance.
You see misinformation spreading	Share the correct source kindly — "I think this one explains it better."	Corrects the issue without confrontation.

🛠️ Simple Ways to Support Others

✅ **Share what you learn.** Talk about scams and safe habits at home, at work, or in your group chats.
✅ **Encourage small wins.** Help someone turn on MFA, or show them how to check a link.
✅ **Be patient.** Everyone learns at a different pace.
✅ **Use plain language.** Avoid terms like “threat actor” or “malware infection.” Say “scammer” or “harmful software.”
✅ **Model good habits.** Others notice when you pause before clicking or use strong passwords.

💡 *You don’t need to be an expert — just someone who cares enough to help.*

📩 When Someone’s Been Scammed

If a friend or relative has been caught in a scam, the most important thing is to stay calm and supportive.

Do this:
1️⃣ **Reassure them** — anyone can be tricked.
2️⃣ **Stop further loss** — change passwords, block accounts, and contact banks if money was taken.
3️⃣ **Report it** — forward phishing emails to report@phishing.gov.uk, or text scams to **7726**.
4️⃣ **Encourage recovery** — help them check devices for malware and talk about what to watch for next time.

⚖️ Avoid blame — the goal is to rebuild confidence, not shame.

Learn & Try

Q1 — What's the best way to help someone who fell for a scam?

A. Tell them it was obvious
B. Help them secure their accounts
C. Share their mistake publicly as a warning
D. Ignore it — they'll learn next time

Q2 — How can you make tech conversations easier?

A. Use short, familiar language
B. Overload with detail
C. Avoid helping to stay out of it
D. Assume they already know

Q3 — Why is listening important in cyber support?

A. It lets people feel heard and safe
B. It wastes time
C. It hides your lack of expertise
D. It's only for professionals

Quick Wins

✅ Listen before you explain.
✅ Share new scams or tips with those around you.
✅ Offer calm help when someone's worried.
✅ Encourage privacy and patience, not panic.
✅ Be the example others follow.

Confidence Check

☐ I can talk about scams without blame or fear.
☐ I know how to help someone recover from a phishing attack.
☐ I use simple, clear language when explaining cyber safety.
☐ I share safe habits with my friends, family, or colleagues.

Section 7:

Everyday Confidence

Staying secure starts with staying calm.

💬 Why Confidence Matters

Cybersecurity can feel overwhelming — constant warnings, new scams, endless updates. But real safety doesn't come from knowing everything; it comes from knowing how to *react* when something happens.

Confidence means being aware without being afraid. It's the quiet habit of pausing, checking, and acting calmly — even when something seems urgent.

You don't need to be fearless — just steady.

⚖️ What Cyber Confidence Looks Like

Confident Habits	What It Means in Practice
Pausing before reacting	You take a moment before clicking, replying, or sharing.
Checking, not guessing	You verify through official apps or websites.
Learning continuously	You stay curious, not anxious, about new scams.
Helping others	You pass on knowledge calmly and kindly.
Recovering, not panicking	If something goes wrong, you take steps — not blame.

💡 *Confidence is a skill. It grows each time you handle something calmly.*

If Something Goes Wrong

Even the most careful people make mistakes — that's okay.
Here's what to do if you think you've clicked, downloaded, or shared something risky:

1. **Stop** — don't click again or reply further.
2. **Disconnect** — turn off Wi-Fi or mobile data if you suspect malware.
3. **Change your passwords** for key accounts (email, banking, social).
4. **Turn on MFA** if it wasn't already active.
5. **Scan your device** with antivirus or security tools.
6. **Report it**:
   - Email scams → report@phishing.gov.uk
   - Text scams → forward to **7726**
7. **Talk about it** — with a friend, colleague, or family member.

Mistakes don't define you. Your response does.

Building Daily Confidence

- ✅ **Keep learning:** Read one new cyber tip a week.
- ✅ **Review your settings:** A five-minute privacy check makes a difference.
- ✅ **Stay calm under pressure:** Urgent messages lose power when you pause.
- ✅ **Trust your instincts:** If something feels off, it probably is.
- ✅ **Celebrate progress:** Every scam spotted is a success.

Confidence is built one safe decision at a time.

Learn & Try

Q1 — What's the first step if you think you clicked a scam link?

A. Panic and delete everything
B. Stop, disconnect, and assess calmly
C. Ignore it — it'll be fine
D. Post online for advice

Q2 — What makes someone "cyber confident"?

A. Never making mistakes
B. Being calm, informed, and willing to learn
C. Knowing every new scam by heart
D. Avoiding all technology

Q3 — What should you do if you feel embarrassed after a scam?

A. Keep it secret
B. Delete your accounts
C. Talk to someone you trust
D. Pretend it didn't happen

Quick Wins

✅ Take five minutes each week to review privacy or security settings.
✅ Keep your devices and apps updated.
✅ Share what you learn with one other person.
✅ Treat every alert as information, not panic.
✅ Remember — calm is your strongest defence.

Confidence Check

☐ I know what to do if I click a scam link.
☐ I understand that confidence grows with practice.
☐ I stay calm when something looks suspicious.
☐ I share what I learn with others.

Section 8:

Quick Reference & Glossary

Your one-page reminder of key actions, contacts, and terms.

Quick Response Checklist

1. **Pause.** Don't click, reply, or share anything further.
2. **Check the sender.** Look at the email or phone number carefully.
3. **Change your passwords.** Start with your email and bank accounts.
4. **Turn on MFA.** Add that second layer of security.
5. **Scan your device.** Use antivirus or your built-in security settings.
6. **Report it:**
   - Forward phishing emails to **report@phishing.gov.uk**
   - Forward scam texts to **7726** (free in the UK)
7. **Talk to someone.** You're not alone — scams happen to everyone.

Common Warning Signs of a Scam

🚨 Sign	What It Means
Urgency ("Act now or lose access!")	They want you to rush.
Fear ("Your account has been locked.")	They want you to panic.
Reward ("You've won!")	They want you to click.
Unusual sender address	Check the real domain — small changes hide fakes.
Strange links or attachments	Don't open unless you're expecting them.

Safe Habits Summary

✅ Use **three random words** for passwords.
✅ Turn on **multi-factor authentication (MFA)**.
✅ Keep **devices updated** and clean.
✅ **Back up** data to cloud and drive.
✅ **Pause before clicking** any unexpected link.
✅ **Check privacy settings** regularly.
✅ **Talk about cyber safety** with others.

Small actions done often make the biggest difference.

Glossary — Plain English Cyber Terms

Term	What It Means
Phishing	Fake messages designed to trick you into sharing information.
MFA (Multi-Factor Authentication)	A second step — like a code or app prompt — that proves it's really you.
Malware	Harmful software that can steal data or damage your device.
Data Breach	When a website or service leaks or loses user data.
Password Manager	A secure app that remembers unique passwords for every site.
Ransomware	A type of malware that locks files until money is paid.
Two-Step Verification	Another name for MFA.
Social Engineering	When someone manipulates or tricks you instead of hacking you.
Spoofing	Faking a phone number, email address, or website to look legitimate.
Backup	A second copy of important data saved somewhere else.

Section 9:

Your Progress & Reflection

Look back, recognise growth, and keep building confidence.

What This Section Is For

You've learned practical skills, spotted scams, and strengthened your habits — but the most important change is how you *think* about staying safe online. Cyber confidence isn't a one-time goal; it's a small, steady habit that grows every day you practise it.

Use these pages to reflect on what's changed, track your confidence, and plan what you'll do next.

Confidence Scale

Having now read the guide, circle where you feel you are:

1. I'm still learning the basics.
2. I know some key steps but forget them sometimes.
3. I use good habits most of the time.
4. I feel calm and capable when something looks suspicious.
5. I'm confident enough to help others.

💡 *Confidence grows with practice — revisit any section when you want to refresh or teach someone new.*

✅ Your Progress Checklist

Tick what applies — this is your reminder of how far you've come.

Passwords & Logins
☐ I use strong, unique passwords for important accounts.
☐ I've turned on MFA wherever possible.
☐ I know how passwords get guessed or stolen.

Scams & Phishing
☐ I can spot scam messages and phishing attempts.
☐ I know how to report scams safely.
☐ I pause before clicking links or replying to strangers.

Messaging & Links
☐ I check links before I tap or click.
☐ I know how to verify if a message is genuine.
☐ I help others recognise suspicious DMs.

Device & Data Care
☐ My devices update automatically.
☐ I keep at least one backup of my important files.
☐ I only install apps from trusted stores.

Online Privacy
☐ I've reviewed my social-media privacy settings.
☐ I limit what personal info I share publicly.
☐ I've disabled unnecessary app tracking.

Helping Others
☐ I've shared what I've learned with someone else.
☐ I listen without judgment when someone needs help.
☐ I know how to report scams or guide others calmly.

Everyday Confidence
☐ I stay calm when something looks suspicious.
☐ I know what to do if I click a scam link.
☐ I keep learning a little at a time.

✍ Reflection Prompts

Take a few minutes to jot down your thoughts.

Name something you feel you've learned from reading this guide.

Which new habit are you looking forward to building?

Who could you help or share this knowledge with next?

What's one area you'd like to learn more about?

Certificate of Completion

Congratulations! You've completed the **Learn Cyber Safety Basics** workbook**.**

By working through these sections, you've shown commitment to protecting yourself and others online.

You've learned how to:

✅ Spot scams and phishing attempts
✅ Strengthen passwords and devices
✅ Manage your privacy and data
✅ Support others with calm confidence

You are now a **Cyber Shoulder** — someone who can help others stay safe, aware, and empowered online.

Name: _____

Date: _____

Trainer: _____

Certificate ID: CYB-SAFE-2025-E001